Christopher J. Schatz, OSB No. 915097
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: chris_schatz@fd.org

Ruben L. Iñiguez
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: ruben_iniguez@fd.org

Attorneys for Hock Chee Khoo

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

HOCK CHEE KHOO, et al.,

Defendants.

CR 09-321-KI

MEMORANDUM OF ARGUMENT RE MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP AND EXTERNAL HARD DRIVE.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

MISCELLANEOUS

Defendant Hock Chee Khoo, through his attorneys of record, Ruben L. Iñiguez and Christopher J. Schatz, respectfully submits the points and authorities hereinafter set forth as Mr. Khoo's argument with respect to the Motion To Exclude Images Of The Wu Laptop And External Hard Drive [Docket No. 34]. In accordance with Rules 901, 1001, 1002 and 1003 of the Federal Rules of Evidence, and pursuant to the afore-referenced motion, Mr. Khoo has moved the Court to exclude from evidence all digital images taken of the laptop computer hard drive used by Shengbao "Jesse" Wu while employed by The Hoffman Group (hereinafter referred to as the "Wu laptop"). The grounds for said motion are as follows:

1. The government has failed to establish a sufficient nexus between the images contained in the Acronis backup file created by Mark Hansen (hereinafter referred to as the "Acronis image" and "Acronis backup copy") and/or the Federal Bureau of Investigation's Forensic Tool Kit EnCase image (hereinafter referred to as the "Wu Laptop image") and the actual data content and configuration of digital images on the Wu laptop, to support the government's claim that the former images accurately represent the data on the Wu laptop as such existed prior to the seizure of that computer by Drew Hoffman on October 17, 2006. The Acronis backup copy and Wu Laptop images should therefore be excluded due to lack of authentication under Rule 901.

2. Following the seizure of the Wu laptop on October 17, 2006, substantial spoilation of the data on the computer took place rendering it impossible to authenticate the data contained in the Acronis backup copy and Wu Laptop images as being identical to the data contained on the Wu laptop prior to its seizure.

3. The Acronis backup copy and Wu Laptop images are not sufficiently accurate reproductions of the data content and configuration on the Wu laptop to qualify as admissible duplicates as required by Rule 1001. Therefore, said images should be excluded from evidence pursuant to Rule 1002.

4. Even if the Acronis and Laptop images were to qualify as duplicates, they are subject to exclusion under the exceptions noted in Rule 1003, because substantial questions pertaining to the authenticity of said images and the manner of their creation exist.

STATEMENT OF FACTS[1]

A. The Hoffman Group's Initiation Of Investigation Activity By The Federal Bureau Of Investigation.

According to Lawrence Andrew Hoffman, in September 2006, his company, The Hoffman Group, had a popular product, the Lambo Door Kit.[2] Hoffman observed that this product was being sold by an unknown entity on eBay. RT 53.[3] According to Hoffman, "we were concerned about it because the ability of that product's – the availability, I guess you would say, of that product was

[1] The Statement of Facts hereinafter set forth is drawn from the testimony and evidence presented during the course of the motions hearing conducted on November 16, 2010, and from discovery received from the government to date. References to the reporter's transcript of the November 16 proceedings are herein designated "R.T." followed by appropriate page number(s).

[2] Litigation pertaining to the ownership of patent rights with respect to this product is currently ongoing in the Southern District of California. RT 54.

[3] According to FBI Special Agent Phil Slinkard, Hoffman regularly scoured the Internet, and more particularly eBay, for the purpose of determining whether his company's parts were being infringed on and manufactured by others. RT 90. On August 25 or 26, 2006, Hoffman noticed that an eBay auction was being conducted with respect to the Lambo Door Kit. This kit was being sold by a company located in West Linn, Oregon, known as sales@cleanlineauto.com. RT 90.

hard to come by." RT 53. Hoffman also was experiencing delay in obtaining this product from the factories in China that were manufacturing the Hoffman company's products, and shipments of Hoffman company products had been delayed. RT 53.

Hoffman contacted his legal counsel, John Ramig, and commenced an investigation. RT 54. Subsequently, a company by the name of JES, LLC, was identified as the source of the Lambo Door Kits that Hoffman had observed being offered for sale on eBay by an entity not related to his company. Hoffman also found out that the employees of JES were current and former employees of his company. RT 55. One of the individuals so identified was Jesse Wu, Hoffman's key contact person in China. RT 54-55.

Having identified Wu as possibly being the source of the problem with the Lambo Door Kit, attorney Ramig contacted the FBI. RT 55. Hoffman then directed Wu to return to the United States and to bring his laptop computer with him. RT 56.[4]

Hoffman testified that he did not know whether the FBI was contacted with respect to Wu's return to the United States. RT 57. However, during an interview with Hoffman on September 12, 2006, SA Slinkard was advised that Wu was expected to return to the United States on or about October 17, 2006. RT 92.[5] Indeed, Hoffman told SA Slinkard that Wu was going to arrive in Portland on Northwest Airlines at 8:05 a.m. on October 17. RT 92.[6]

[4] According to Hoffman, he told Wu, "We would like you to return to go through some training." RT 58.

[5] SA Slinkard's report of his interview with Hoffman was received into evidence as Defendant's Exhibit 8. RT 102. A copy of this report is attached hereto as Exhibit A.

[6] No plan was made by the FBI to interview Wu upon his return to the United States. SA Slinkard explained that he did not formulate such a plan because he was not the case agent on the case. According to Slinkard, the case agent was George Chamberlain. RT 93.

B. The Seizure Of The Wu Laptop.

On October 17, 2006, Hoffman picked Wu up at the airport and then drove to The Hoffman Group office on Oak Street. Wu was taken into the building and led upstairs to an office where he was introduced to Mark Hansen. RT 58. Wu was told to give his computer to Hansen because Hansen was going to update it. RT 59. Wu handed his computer over to Hansen. RT 59.

When Wu turned his computer over to Hansen, he specifically stated to Hansen, "Don't touch this file. Don't touch this particular spot." RT 77. After Wu left the room, Hansen copied that file and Hoffman later found this file, called "Private," on the laptop. RT 77.

Once the computer was taken into Hansen's custody, Hoffman took Wu to the shop area where Wu was introduced to a lawyer from attorney Ramig's office. RT 60-61. Another person was also present whose purpose was to "provide Mr. Wu with some papers concerning the civil matter." RT 61.[7] There was no Chinese interpreter nor was any representative of the government present. RT 62.

After Hansen transferred a copy of the Wu laptop hard drive to a USB external hard drive using Acronis software, the laptop was given to Hoffman. RT 63. It was now late at night, and Hoffman recalls opening the laptop and looking in the laptop for any information that could shed light on the situation that was going on. RT 63.

[7] On October 16, 2006, Hoffman filed a civil suit in Multnomah County Circuit Court against Wu, JES Suppliers, LLC, and defendants Soutavong and Khoo, seeking injunctive relief and monetary damages. A copy of the complaint in Multnomah County Circuit Court Case No. 0610-10861 is attached hereto as Exhibit B. It is requested that the Court take judicial notice of the filing date of this litigation pursuant to Federal Rule of Evidence 201(b)(2).

For two days the laptop was continuously in Hoffman's possession. RT 64, 78. On a number of occasions Hoffman turned the laptop on and booted it up. RT 64.[8] During this time period, Hoffman "could have" moved files from one location on the laptop hard drive to another. RT 71. Hoffman denied deleting any data from the laptop. RT 71. Hoffman also denied running the defragmentation utility:

> Q. Did you delete data from the laptop during that period of time?
>
> A. I don't recall deleting anything.
>
> Q. Now, there's a subtle point between not recalling and I did not. So I just want to be clear. Is it your testimony that you did not delete any electronic data from the laptop during the period of time it was in your possession?
>
> A. That is correct.
>
> Q. Did you run the defragmentation utility?
>
> A. No, I did not.

RT 64. No one else had access to the computer during the time that Hoffman had it in his possession. RT 65.

Hoffman acknowledged that attorney Ramig had assisted him in setting up his company's business activities in China. RT 67. With respect to those business activities, Hoffman was asked

[8] The Wu laptop used a Windows operating system. RT 75. Hoffman testified that he is a Mac guy (*i.e.* a user of the Apple Macintosh computer operating system) not a Windows guy. RT 75. Hoffman testified that he is "not fluent in Windows" and that he is "uncomfortable" with the Windows operating system. RT 81. Nevertheless, he proceeded to operate the Wu laptop for a period of several days. RT 81.

some questions concerning e-mail communications between himself and a Richard X concerning Hoffman's avoidance of tariffs on products manufactured for his company in China:[9]

> Q. And your response to the statement from Richard X, I guess it is, to you, "I was informed by Jess that you need us to separate the CIF price in the invoice to the FOB price plus freight cost and insurance so that you can pay less tariff when declaring customs," what was your response? Would you read that into the record?
>
> A. My response was, "Please just make the same half invoice and add the value to the freight and insurance."
>
> Q. And there's a response to that by, again, further down, because it says in the e-mail from Richard to you, "According to our experience with China customs, customs will levy tariff according to the unit price of each item. If we do as you are requiring, the unit price of every items will change each time due to the freight cost and insurance changes each time. If so, how do you explain to your customs? Will it cause any problem to you?" That's what Richard is saying to you, correct?
>
> A. Correct.
>
> Q. And what was your response? Would you read that into the record.
>
> A. My response was, "No, because we don't pay on the freight and insurance."
>
> Q. And you recognize these e-mail transmissions as containing data that you participated in generating; is that correct?
>
> A. Could you repeat that?
>
> Q. These are e-mail communications between you and other individuals. You recognize them as such?
>
> A. Yes.

RT 70-71. According to Hoffman, "[w]hen we realized that there was an issue with the tariffs, I engaged Mr. Ramig to review it and advise how to solve it so we can get everything squared away."

[9] The e-mail communications are set forth in Defendant Khoo's Exhibits 6 and 7. These exhibits were received by the Court. RT 71. Copies of Defendant's Exhibits 6 and 7 are attached hereto as Exhibit C.

RT 73. The end result was that Hoffman ended up paying money back to customs for tariffs. RT 74.[10] Hoffman did not undertake to clear up his tariff problem until sometime after he had initiated the Multnomah County civil litigation. RT 79-80. There was no federal investigation. RT 74.[11]

C. Delivery Of The Wu laptop And The USB External Hard Drive Containing The Acronis Back-Up Copy To The FBI And The Creation Of The FTK EnCase Images.

On October 20, 2006, SA Slinkard met Hoffman at the Northwest Regional Computer Forensic Laboratory (NWRCFL). RT 99. Hoffman brought the Wu laptop with him at the request of SA Slinkard. RT 46.[12] Hoffman told SA Slinkard that he had turned on the computer and examined some of its contents. RT 99. Hoffman had examined the folder that was labeled "Private," as well as other files. RT 99.[13]

[10] Hoffman does not know when the repayment of tariffs was made nor how much was repaid. RT 80.

[11] According to FBI Special Agent George Chamberlain, during the course of interaction with Brian Emerson, and/or Emerson's attorney, Jeff Edelson, information pertaining to tariff fraud by Hoffman was revealed to him. RT 39. SA Chamberlain was the "case agent" on the Hoffman company investigation. RT 93. SA Chamberlain did not require Hoffman to produce invoices with respect to products he had imported into the United States in order to determine whether the allegations concerning tariff fraud were accurate. RT 40. There was some discussion between Agent Chamberlain and personnel of the United States Attorney's Office concerning the tariff fraud accusation, but no investigation of the tariff fraud accusation was initiated. RT 40-41. SA Chamberlain was subsequently advised that Hoffman had made repayments with respect to tariff costs, but he never verified the claim or determined how much Hoffman repaid. RT 48.

[12] According to SA Chamberlain there was no communication between the FBI and Hoffman between September 13 and October 20, 2006. RT 46. Nor did the FBI become aware that Hoffman had possession of the Wu laptop until October 20, 2006. RT 46.

[13] SA Slinkard acknowledged in his testimony that Hoffman "did spend a fair amount of time looking through files." RT 99. Hoffman also created a folder on the laptop labeled "QQ." RT 99.

While Hoffman was at the Northwest Regional Computer Forensic Laboratory, SA Slinkard observed him make a copy of the one of the files on the Wu laptop hard drive. RT 101. Notwithstanding Hoffman's claim as to a lack of familiarity with the Windows operating system on the laptop, Hoffman did not appear to experience any difficulty copying from the laptop hard drive to his USB device. RT 102.

Forensic images of the Wu laptop and the USB external hard drive containing the Acronis backup copy were subsequently created between November 3, 2006, and November 6, 2006. RT 158. The forensic imaging was performed by FBI Special Agent Joel Brillhart. RT 161-62.

D. Overview Of The Testimony Of Forensic Computer Expert Michael Bean Regarding The Wu Laptop.[14]

Based on his review of a report prepared by Mark Hansen, Bean was informed Hansen took custody of the Wu laptop computer on October 17, 2006. Hansen located a folder or file on the computer hard drive, named "Private," which he then moved to the computer's desktop. RT 109-110. One of the cornerstones of forensic computer practice is not to alter the state of the data on an item being analyzed. RT 110.

The file system on the Wu laptop hard drive was NTFS.[15] Within this type of file system, file locations are stored and tracked by a Master File Table (MFT). The Master File Table is a master list in the form of a table used to record where files reside on the disc. This master list is the only way a computer is able to locate files to run programs and retrieve or store data. RT 110. By moving the "Private" folder from its original position on the directory tree of the Wu laptop hard

[14] The Court recognized Bean as an expert in forensic computing. RT 107.

[15] NTFS is the standard file system (*i.e.*, architecture) for the operating system for Windows XP.

drive to the desktop of the hard drive, Hansen altered the Master File Table on the Wu laptop hard drive. The "movement of that folder from one place to the other on the disc at a minimum would have changed the data in the master file table relating to the storage location on the disc of where that information resided . . .." RT 110.[16]

Bean was provided two Forensic Tool Kit EnCase images of the Wu laptop computer by the FBI. RT 109.[17] One of the images was of the Wu laptop and one was of a USB external hard drive storage device that held the Acronis software backup copy that had originally been made by Hansen. RT 112.[18] Looking at the Wu laptop computer image, Bean was able to confirm that the Acronis

[16] From the standpoint of forensic computing principles, the first error committed by Hansen was that he turned the Wu laptop computer on. The second error was his movement of the "Private" folder or file. RT 110-11. It is inappropriate, from a forensic computer expert's standpoint, to turn on a computer that is under investigation for the following reason:

> Since simply starting a computer, turning a computer on will invoke the commands to basically activate the operating system on that computer, that operating system is going to start running any predefined scripts. Any things that are supposed to happen on startup are going to run. Therefore, dates and times of information is going to change on the allocated space, and anything that happens to be overwritten or is too large for the current storage is going to overwrite the unallocated space. So many changes can be made to a computer just by simply turning it on.

RT 111.

[17] Forensic Tool Kit (FTK) is a forensic software made by AccessData. RT 108. EnCase, developed by Guidance software, is a format that is used to store hard drive images. FTK has the ability to create images using the EnCase format. Rt 108-09. Thus, in this case, the Forensic Tool Kit software was utilized to create images of the Wu laptop hard drive and the Hansen USB device containing the Acronis backup copy in the EnCase format. RT 109.

[18] Bean found that the NWRCFL computer that had been used to create the FTK images had not been properly calibrated because the creation dates preserved in the images were October 3 and October 5, 2006:

> The forensic software records the date and time of the computer that was used to make the image. In this case, the date and time of the computer that was used to

software had been installed on the Wu laptop hard drive. RT 112.[19] The most immediate impact of installing the Acronis software on the Wu laptop hard drive was that, as a new piece of information coming into the file system, it's "going to override something in unallocated space in order to provide further room for the active data to be stored." RT 112.[20] From a forensic computer examiner's standpoint, it is important to preserve the status of unallocated space when an examination of a hard drive begins. RT 113.

According to Bean, software exists that has been "designed specifically to capture unallocated space as well as allocated space," so as to "authenticate, be able to authenticate that later as not having changed from the time it was collected." RT 113. Imaging software generates a "bit for bit copy . . . that includes allocated as well as unallocated space." RT 113. The Acronis backup software is a program limited to the reproduction of the allocated space (i.e. the space marked in active use by the Master File Table) on a hard drive. RT 113. Moreover, the Acronis backup software does not create an identifying mark, such as a hash value, that provides a means by which to determine whether the files within an Acronis backup copy have been altered, added, or deleted.

> make the image was set to the 3rd, and the other one was set to the 5th, if they used two separate computers, or they did it on two separate dates, one two days after the other.

RT 139.

[19] Bean determined that the Acronis software had been installed on the Wu laptop computer at approximately 1:13 a.m. on October 18, 2006 (China time). RT 132. Based on the logs Bean was able to recover from the FTK Encase Wu laptop computer image, it appeared the Acronis software was run on at least four occasions, three of which failed. RT 132.

[20] Unallocated space is space that the Master File Table is not keeping track of. Unallocated space "contains information that's either been deleted at a prior time or it's just extra space that's not being occupied by files that the ordinary user can access, which would be the allocated space." RT 112-13.

RT 115.[21] Consequently, the Acronis backup software is not recognized as a forensic imaging tool. RT 113-14.

Bean undertook to explain how a computer hard drive functions so as to assist the Court in its understanding of the deficiencies of the Acronis backup copy software. Before a hard drive is employed by a user, the only file data contained on the hard drive is that of the operating system and any programs that have been installed on the hard drive. RT 115-16. When a file is written to the hard drive, the sector(s) on the hard drive involved with that file creation are filled with electronic data. RT 116. Sectors are grouped by the Master File Table (MFT) into clusters for ease of transferability of data. RT 116.

As electronically stored information, a file contains two distinct data components. One of the components is the file content. The other component is the metadata that is specific to the file. RT 116. System metadata is included in a file's electronic data but it is often not immediately visible to a user. System metadata deals with the created dates, the access dates, the written dates, the last written dates, and additional data under the NTFS file system, such as an entry modified date. RT 117. With respect to the importance of metadata, Bean observed: "The metadata helps tie back and confirm what file was where, and I could also track – or anyone could track, for that matter, the history of the file and a lot of useful things from the metadata." RT 117.

Slack space is defined as anything in a sector that is not occupied by current logical data – *i.e.* by data that will be recognized as a file or electronic document by the Master File Table.

[21] A "hash value" is simply a series of numbers produced by a logarithm that generates a digital fingerprint for the content of a file. RT 114. Depending on whether it's an MD5 or SRA-1 hash value, the hash value basically means "how many . . . how many digits are in that digital fingerprint." RT 114. The forensic utility of a hash value lies in the fact that if the electronic content of a file changes, the hash value of the file will also change. RT 114.

RT 118.[22] When a file or electronic document is deleted, the Master File Table will no longer recognize the file as being present. However, the electronic data remains and can be recovered unless and/or until it is overwritten. RT 118. The Acronis backup software copy is not an exact copy of the Wu laptop hard drive because it does not capture unallocated space. RT 120.

In the course of examining the Wu laptop images, Bean found that the Acronis backup copy contained 285 files in a folder called "Lost Files," a folder that had been created by the FBI's FTK imaging software to hold files that could not be resolved back to any specific folder by the FTK imaging process. Pertinently, none of the 285 files contained in the Acronis backup software copy could be found on the FTK Encase image of the Wu laptop computer. RT 122. Based on this discovery, Bean concluded:

> Well, obviously if there's files that exist in the Acronis backup copy that do not exist in the forensic image of the laptop, and the Acronis backup copy was made prior to the image of the laptop, there was some deleting going on on the laptop. So those 285 files, at a minimum, had been deleted prior to the EnCase image being made of the laptop.

RT 122.

Electronically stored information is subject to manipulation and change. For example, it is possible to change the date entries on data so that data that is stored on the computer can be re-dated

[22] The Master File Table groups hard drive sectors into larger clusters for ease of transferability of data. RT 116. "Slack space" is created within a cluster of sectors if the logical data (i.e. user data or program files) does not fill an entire cluster. Slack space is the unused disk space within a cluster. When a logical data file is marked by a user or system action as "deleted," the file remains on the hard drive, but the space it occupies is marked by the Master File Table as available (*i.e.* unallocated space) to which new data can be written. In other words, the data will no longer be present on the Master File Table, its entry will have been deleted, but the data itself is still retrievable using forensic examination tools. When new data is written to that unallocated cluster space, if the new data does not completely overwrite the old data, the remnant of the old data that resides in the slack space of the new data can also be retrieved. RT 118.

to a time prior to its actual creation. RT 123. With respect to the content of the Acronis software backup copy, Bean noted, "There is no way to authenticate that that data today is the same as it was the day it was collected." RT 123.[23]

According to Bean, file metadata is also important to the determination whether electronically stored information has been manipulated. RT 124. File metadata can be lost by deletion if a defragmentation utility is run.[24] After the Acronis backup copy had been made, Bean found evidence that the defragmentation utility had, in fact, been employed on the Wu laptop. Bean explained the effect of running this utility:

> The defragmentation program, also known as defrag, is a utility provided by Windows on all Windows-operating machines. What that utility does is it tries to optimize the system. So it makes the data that is currently in unallocated space that may be fragmented across several sectors, based on the fact that when a file comes in, it just puts data wherever it can fit. So you may -- you have some fragmentation there, and it takes a while to resolve all those different locations. So if you can relate to opening a large file on your computer, usually it takes longer than opening a small file on a computer, and that's why, because you have to resolve all of those different extents of the file. The purpose of defrag is to take the information that is not . . . in the active master file table as being an active file, and moving that information around in the unallocated space to make as many files in -- held contiguously in their clusters versus fragmented. And that's the purpose of it. So it would take information from the bottom of the hard drive or the bottom of the unallocated space and try to move it as close to the top as it could, overwriting what was in the top spot in the unallocated clusters as long as it wasn't allocated for use.

[23] If something was to be changed in the FTK EnCase image, the hash value of the EnCase image will not match up with the hash value of the computer data content as it was on the date the FTK EnCase image was originally made. RT 123. However, as noted previously, the Acronis software does not support hash valuation and therefore it is impossible to tell whether the electronic data content on the USB device was manipulated prior to the time that the FTK EnCase image of that device was made.

[24] By removing the Master File Table records of deleted files and overwriting space marked unallocated, the "Defrag" utility renders deleted file data unrecoverable. *See* Supplemental Declaration Of Computer Forensics Expert Michael A. Bean In Support Of Motion To Exclude Images Of The Wu Laptop Hard-Drive [Docket No. 82], at p. 4.

RT 130-31. Bean determined that the defrag utility had been employed at 11:44 a.m. China time.[25] Converting from China time to Pacific Standard Time, the defrag operation or utility was run at approximately 8:44 p.m. on October 17. RT 131.[26]

Bean was specifically asked to search for two e-mail files or folders on the FTK EnCase Wu laptop image with the extension ".PST." The extension .PST stands for personal storage table which is an Outlook e-mail file. Bean was asked to search for two such files, one labeled 2006 and the other one 2005.

Bean located a "Hoffman 2006" .PST file in deleted space in the FTK EnCase Wu laptop image. RT 127. However, Bean was not able to open it with Outlook. RT 127. Bean was not able to determine from evaluating the file when it had been deleted, nor could he find a "Hoffman 2005" .PST file on the computer. RT 127-28.

With respect to the manipulation of the electronically stored information on the Wu laptop hard drive, Mr. Bean testified as follows:

> From the time the Acronis image was listed to have been created, between that time and the time of the last file on the system that I could see, there were over a thousand files that had either been created, accessed or written to that hard drive from the time that Jesse relinquished control of that to Mark Hansen . . .

RT 128. According to Bean, the use and employment of the Wu laptop hard drive "degraded the amount of unallocated cluster data that I had to work with . . .." RT 129. In addition to activity with respect to the aforereferenced 1000 files, Bean also noticed that the Wu laptop hard drive had been used to conduct web surfing as well as installation of programs. According to Bean, "[A]ll of those

[25] The Wu laptop computer was actually set in its registry to China time. RT 130.

[26] Although he denied employing the defrag utility, Hoffman testified it was "late at night" when he opened and booted-up the Wu laptop on October 17, 2006. RT 63.

things combined had a tremendous effect on the content of the unallocated space and any recoverability of data from there, and even if I do recover it, how much was really there and how much was missing." RT 129.

In conclusion, Bean stated as follows with respect to the forensic integrity of the FTK EnCase images of the Wu laptop and the Acronis backup copy:

> Q. As a computer forensic expert, do you have an opinion as to whether the data contained on the FTK EnCase Wu laptop image has sufficient trustworthiness and integrity that you can say with reasonable certainty that the data as it is now displayed in that image was on the Wu laptop computer when the computer was taken from Mr. Wu on the morning of October 17, 2006?
>
> A. Absolutely not. That data that is contained in the EnCase image that the FBI made has changed. From the time that Wu surrendered that computer, there was overwriting, there was installation of software, there was Web surfing, there was mass deletions, there was a defragmentation ran. There is no way that the data that resides in that image today is the same as it was when it was surrendered by Wu.
>
> Q. As a forensic computer expert, do you have an opinion as to whether the data contained on the FTK EnCase Acronis backup copy image has sufficient trustworthiness and integrity that you can say with reasonable certainty that the data as it is now displayed in that image was on the Wu laptop computer when the computer was taken from Wu on the morning of October 17, 2006?
>
> A. No. The Acronis image, as you can see by the exhibits that we've already shown, the data in that is different. It's missing the unallocated space. The Acronis software has not been tested. It's not accepted in the forensic community as an imaging tool. If anything, it's been advised not to use that as an imaging tool. And there's no unallocated clusters. There's no way that I can recover the 75,000 files. Those same 75,000 files should be recoverable in the Acronis image if the unallocated space existed. It does not. I cannot recover those same files like I did. Even though there was alteration of the laptop that was imaged, I was still able to recover things from unallocated space.

RT 134.

E. The Government's Misleading Attempt At Rebuttal.

In rebuttal to the testimony of Forensic Computer Expert Bean, the government called Portland Police Bureau Officer Steven Johns.[27] Johns testified that he is currently assigned to the Northwest Regional Computer Forensic Laboratory in Portland as a computer forensic examiner. RT 155.

During the 2006-2007 time period, Johns was familiar with a person by the name of FBI Special Agent Joel Brillhart. RT 156. According to Johns, when a case is completed at the laboratory, both a peer review and an administrative review is conducted. RT 155. The peer review is a review that is done by people who are technically knowledgeable about the subject the examiner has participated in. In this case, "the peer review was done by a computer forensics examiner." RT 155. Johns conducted the administrative review, which he described as "more of a cross the T's and dot the I's review to make sure the case numbers are properly entered and the documentation is properly formatted." RT 155-56.

Based on his review of NWRCFL records, Johns testified that the Acronis backup copy and the Wu laptop were initially checked into the Evidence Control Facility on November 1, 2006. RT 157.[28] The Wu laptop and the Acronis backup copy were later checked out again for imaging

[27] No attempt to qualify Johns as an expert witness was made, and the Court did not recognize Johns as an expert witness.

[28] It should be noted that in his examination of Johns, AUSA Nyhus repeatedly referred to the Acronis backup copy made by Hansen as the "Acronis image." RT 157. Insofar as the Acronis software did not generate a byte-for-byte (*i.e.*, physical content) reproduction of the Wu laptop hard drive disk space, so as to reproduce all electronic data in allocated as well as unallocated sector space, referring to the product generated by use of the Acronis backup copy software as an "image" is improper.

on November 3, and returned to the evidence room on November 6, 2006. RT 158.[29] Johns does not know who had possession of the Acronis backup copy and the Wu laptop from October 20 to November 1. RT 159-60.[30]

Based on his review of SA Brillhart's file and materials, Johns did not find any indication that the NWRCFL's forensic computer imaging equipment had not been properly calibrated. RT 161. In his opinion, SA Brillhart had concluded his "examination within acceptable guidelines." RT 161.

Testifying on cross-examination, Johns acknowledged that the Acronis backup copy software is not a standard forensic imaging tool that is used at the Northwest Regional Computer Forensic Laboratory. RT 164. Johns has never used the Acronis backup software to make a forensic image, and he would not use such software to make a forensic image. RT 164. Johns did not personally examine the FTK EnCase images of the Wu laptop computer hard drive or the Acronis software backup copy. RT 164-65.

Johns had not been advised before he was called to court that a concern had arisen with respect to the calibration of the NWRFCL's equipment that could have resulted in misstating the dates of creation for the images. RT 165. Johns was unable to state whether, given the technology

[29] A report of this imaging activity was generated. RT 158. A request for production of this report and all related NWRFCL file documentation has been tendered to the government.

[30] AUSA Nyhus had clearly been under the impression that the Wu laptop and the Acronis backup copy contained on Hansen's USB external hard drive had been checked into the NWRFCL on October 20 or 21. RT 157, 159. He was surprised by John's answer that the records of the Evidence Control Facility disclosed that the Wu laptop and the Acronis backup copy had not been checked into the Evidence Control Facility until November 1, 2006. RT 159. No explanation for this breakdown in the chain of custody pertaining to these items has been tendered by the government to date.

utilized by SA Brillhart in creating the FTK EnCase images, a date entry was embedded in the images. RT 165-66.[31]

The limited scope and substance of Johns' testimony is disclosed by the following question and answer sequence:

> Q. So as you sit here today, separate and apart from your review of paperwork, you're not able to tell us what the FTK EnCase Wu laptop image contains with respect to a creation or acquired date; is that correct?
>
> A. Correct.
>
> Q. If Sergeant Brillhart – or Special Agent Brillhart erred, and his paperwork is incorrect, you are unable to verify the creation or acquired date of the FTK EnCase images; isn't that correct?
>
> A. I reviewed his notes, and whatever he had as a date that he did the acquisition is what I went on.
>
> Q. So you're relying solely on Special Agent Brillhart's notes?
>
> A. Yes.
>
> Q. And not on any examination of the imaged data itself?
>
> A. Correct.

RT 167-68.[32]

[31] In this regard, Johns stated, "So I'm not familiar with that methodology, although it is approved and acceptable. I do not know whether or not there is embedded information within those files. So I can't answer that right now." RT 166. Again, referring to the software used by SA Brillhart to create the images, Johns admitted: "I do have some expertise with the software he used to create EO1 images. However, I do not have the expertise to let you know whether or not the metadata information within the EO1 images contains information that would tell you the acquired date of those particular images in question." RT 166-67.

[32] Johns also reviewed the peer reviewer's notes pertaining to SA Brillhart's activities in imaging the Wu laptop and the USB external drive containing the Acronis backup copy. RT 168.

On redirect, AUSA Nyhus attempted to have Johns suggest to the Court that the "hash values" of the "images" were identical:

> Q. There has been some question about or some talk about what an MD5 hash is. Did you compare the hash values of the images before and after?
>
> A. I did.
>
> Q. Were all before hash values compared to and against each other?
>
> A. The images files in the case notes, yes. I compared both before and after.
>
> Q. So the hash values, did they match?
>
> A. Yes, they did.

RT 170.

On recross, Johns admitted that the hash values he was referring to were not hash values associated with the content of the Wu laptop and the Acronis backup copy, but simply the hash values associated with the forensic images generated by SA Brillhart:

> Q. In terms of the hash values that you compared, is it not the case that those are the hash values simply of the imaged files themselves, not of the content?
>
> A. Yes.
>
> Q. And those – that analysis you did with respect to the hash values is simply of the imaged files themselves, that was done by looking at the paperwork; is that correct?
>
> A. Correct.

RT 171.[33]

[33] As explained by Forensic Computer Expert Bean, when a forensic image is created, there is a hash value that is constructed on that image. RT 114. If the hash value connected to an image

ARGUMENT

DESPITE SERIOUS CONCERNS WITH RESPECT TO SPOLIATION OF EVIDENCE AND CHAIN OF CUSTODY, THE GOVERNMENT HAS FAILED TO ADDUCE SUFFICIENT EVIDENCE TO ENABLE THIS COURT TO REACH A PRELIMINARY DETERMINATION REGARDING THE AUTHENTICATION OF THE WU LAPTOP AND ACRONIS BACK-UP COPY IMAGES, CONSEQUENTLY THOSE IMAGES MUST BE EXCLUDED FROM EVIDENCE.

A. Where Spoliation Of Electronic Evidence Appears To Have Taken Place, The Proponent Of The Admission Of Such Evidence Must Submit Evidence Of Sufficient Facts To The Court To Enable The Court To Make A Preliminary Determination That The Electronic Evidence Is Trustworthy.

Evidence may be admitted only if the court "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." F.R.E. 901(a). The key purpose of the authentication requirement is to ensure that only genuine and trustworthy evidence is considered at trial. *See, e.g., United States v. Panaro*, 266 F.3d 939, 951 (9th Cir. 2001) (for evidence to meet authenticity requirement, trial court "must be satisfied that it is 'accurate, authentic, and generally trustworthy'") (citations omitted). This inquiry is a threshold to introduction of evidence, not simply a matter bearing on the weight to be afforded it. *See United States v. Logan*, 949 F.2d 1370, 1377-78 (5th Cir. 1991); *United States v. Stearns*, 550 F.2d 1167, 1170 (9th Cir. 1977) (before

changes, the forensic examiner knows that the content of the image or file has also changed. On the other hand, if the "hash value remains the same, it means that the data remain the same from the time I collected it." RT 115. The thrust of Johns' testimony concerning the hash values of the "images" was simply that there did not appear to have been any change in the content of the images subsequent to their creation. No hash value analysis was ever performed comparing the hash values associated with the contents of the Wu laptop, as they existed on October 17, 2006, prior to the laptop's seizure by Hoffman, and the hash values of the subsequently created FTK EnCase images.

photograph can be admitted, it must be authenticated as technically accurate representation of scene photographed).[34]

While in many respects the issues pertaining to the authentication of a paper record and the authentication of electronic record data are similar, there are also important differences:

> Authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained: one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file. Fed.R.Evid. 901(a).
>
> **Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.**
>
> In the case of a paper record, the inquiry is into the procedures under which the file is maintained, including custody, access, and procedures for assuring that the records in the files are not tampered with. The foundation is well understood and usually is easily established. *See* Edward J. Imwinkelried, EVIDENTIARY FOUNDATIONS §4.03[1] (5th ed.2002) ("Imwinkelried"); 5 Weinstein §900.07[1][b][i].
>
> **The paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records.** Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be.

[34] Federal Rule of Evidence 402 provides that, except for certain specified limitations, all relevant evidence is admissible, and all irrelevant evidence "is not admissible." Federal Rule of Evidence 401 declares that to be relevant, evidence must have a "tendency to make any fact that is of consequence to the determination of a matter more probable or less probable than it would be without the evidence." An item of evidence can perform this function in the ascertainment of the truth only if it is in fact what its proponent claims it to be. Accordingly, "authentication is a mandatory first step in determining evidence to be relevant." 5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* § 900.06[1][b] (2d ed. 2005). Evidence that is not what its proponent claims it to be is irrelevant and inadmissible under Rule 402. *Id.*

In re Vee Vinhnee, 336 B.R. 437, 444 (9th Cir. 2005) (footnotes omitted) (emphasis added).[35]

That the difference in format, as between paper and electronic records, can present unique challenges with respect to admissibility, has been recognized.

> *Use at trial*. In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. **The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.**
>
> The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings, so that challenges to the evidence are not made for the first time at trial. . . ..

MANUAL FOR COMPLEX LITIGATION (Fourth) §11.446 (2004) (emphasis added); *see also In re Vee Vinhnee*, 336 B.R. at 445 ("[D]igital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to assure the continuing integrity of the records.").

[35] Computer-based documents are distinct from hard-copy paper documents in two fundamental ways:

> First, computer-based documents contain metadata that is not revealed in a hard-copy printout of the document . . ..
>
> Second, "deleted" computer-generated documents are not irretrievably lost (at least for a potentially long time), unlike missing, destroyed, or (for the most part) shredded paper documents. Recovering deleted electronic documents is often possible, although the process may sometimes be time consuming and costly . . ..

5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* §900.01[3] (2d ed. 2005).

Where there is a genuine concern that computer-based electronic evidence may have been altered or manipulated, an additional degree of scrutiny by the courts is appropriate. *See* Saltzburg, Martin & Capra, *Federal Rules of Evidence Manual* §901.02[3] (9th ed. 2006) ("[W]hen it comes to the question of whether the Judge must make a preliminary determination before admitting evidence, as opposed to simply deciding there is enough for the jury to decide whether to rely on the evidence, the best reading of Rule 901 would be to follow a case-by-case approach and to demand a more substantial foundation where the circumstances might create a suspicion that evidence is altered or fabricated."). In order to warrant this heightened scrutiny, the objecting party must make a showing that raises serious concerns about authenticity. *See United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (even if web postings, in which white supremacists took responsibility for racist mailings, qualified for business records hearsay exception, they were "inadmissible if the source of information or the method or circumstances of preparation indicate a lack of trustworthiness;" thus, proponent failed to authenticate web postings, since there was some evidence that she had the motive and technological ability to place them on the groups' web sites herself); *see also United States v. Clonts*, 966 F.2d 1366, 1368 (10th Cir. 1992) ("[I]f the evidence is open to alteration or tampering, or is not readily identifiable, the trial court requires a more elaborate chain of custody to establish that the evidence has not been tampered with or altered.") (citations omitted).[36]

[36] Chain of custody is a component of authentication. *See, e.g., United States v. Salcido*, 506 F.3d 729, 733 (9th Cir. 2007) ("[T]he government properly authenticated the videos and images under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers.").

B. As A Condition Precedent To Authentication Of The Logical Content Of The FTK EnCase Wu Laptop And Acronis Back-Up Copy Images, The Government Must Also Authenticate Those Images As Constituting True Reproductions Of The Logical And Physical Content Of The Wu Laptop As It Existed Prior To Its Seizure By Hoffman On October 17, 2006.

When the origin of a record or document offered into evidence is the electronic data on a computer, in addition to the basic foundation requisite to admissibility of that record or document, an additional authentication foundation regarding the computer and software utilized to create that record or document must be established in order to assure the continuing accuracy of the record or document in question. *In re Vee Vinhnee*, 336 B.R. at 442.[37] The situation in the instant case is even more complicated in that the government seeks to adduce documents taken, not from the original Wu Laptop, but from second-generation sources – the FTK EnCase Wu Laptop image and the FTK EnCase Acronis backup copy image. Thus, in addition to authentication of the Wu Laptop software systems, a third tier of complexity and authentication must be addressed with respect to authentication of the electronic data contained in the images. This third tier requires that the images themselves be authenticated as constituting identical reproductions of the Wu Laptop hard drive electronic data content as such existed at the time the Wu Laptop was seized on October 17, 2006.

Federal Rule of Evidence 901(b)(9) "was designed to encompass computer-generated evidence." *In re Vee Vinhnee*, 336 B.R. at 446. Rule 901(b)(9) provides:

[37] There are two types of software – systems programs (which govern the operation of the computer) and application programs (which put the computer to a particular use, such as to create a balance sheet or recreate an event) – both of which must be authenticated if electronically created and/or stored data is to be admissible. *See* Gregory P. Joseph, *A Simplified Approach To Computer-Generated Evidence and Animation*, 43 N.Y.L. Sch. L. Rev. 875, 884 (1999-2000).

> (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.[38]

While the theory of operation and general reliability of computers and electronic software is often a subject of judicial notice, theory and general reliability are only a part of the foundation necessary to authenticate an electronically reproduced record. Among other requirements, in the instance of electronically preserved documentation, the procedures utilized in such preservation must contain "built-in safeguards to ensure accuracy and identify errors." *In re Vee Vinhnee*, 336 B.R. at 446.[39]

Forensic Computer Expert Michael Bean testified that neither the FTK EnCase Acronis image nor the FTK EnCase Wu laptop image had sufficient trustworthiness and integrity to allow him to say with reasonable certainty that the data content of those images reproduced the data that was on the Wu laptop at the time Hoffman seized it on October 17, 2006. In response to AUSA Nyhus' attempt at a simplistic analogy comparing two pieces of paper – one taken from the Acronis backup copy image and one from the Wu laptop image – Forensic Computer Expert Bean repeatedly

[38] The Advisory Committee Note to Rule 901(b)(9) describes the scope of application of this subpart as follows:

> Example 9 is designed for situations in which the accuracy of a result is dependent upon a process or system which produces it. X rays afford a familiar instance. Among more recent developments is the computer, as to which *see Transport Indemnity Co. v. Seib*, 178 Neb. 253, 132 N.W.2d 871 (1965); [other citations omitted]. Example (9) does not, of course, foreclose taking judicial notice of the accuracy of the process or system.

[39] As noted in *In re Vee Vinhnee*, the "built-in safeguards to ensure accuracy and identify errors" "subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the **continuing integrity** of the records." 336 B.R. at 446-47 (emphasis added).

pointed out that the lack of integrity and functionality associated with the Acronis back-up copy software rendered any such attempted comparison highly suspect:

> Q. On the hypothetical, if I created a copy of something and used the contents to prove the content, and they're identical one to the other, what does it matter if one is not a forensic image to the other?
>
> A. That's what I'm telling you. You cannot – I cannot confirm the starting digital fingerprint of the Acronis, the content that's contained in the Acronis image. So even though a spreadsheet that may be named the same as it is in the EnCase image, I don't know that the two content are the same because this may have changed. I can't confirm that it did or it didn't because there was no hash values made when the image was made. On the other hand, the EnCase image, I can tell that it didn't change, but is it the same? Did they put it on here after? Who knows? I can't tell because it wasn't imaged correctly from the beginning.
>
> . . . .
>
> Q. I guess I'm going back to my question. It says"Mr. Bean" here and it says "Mr. Bean" there. Okay?
>
> A. Understand.
>
> Q. Mr. Bean says Mr. Bean. These two look like identical copies. They're not forensic images of each other but they're identical copies?
>
> A. They're probably not --
>
> Q. Does it matter, then, sir, to the content of the assertion of Mr. Bean and Mr. Bean that 256 forensic copies are -- files are missing?
>
> A. Yes, it does matter. That's what I'm telling you. The content from the files, the "Mr. Bean" file and the Acronis image cannot be verified from the time it was made. So I cannot take that and compare the digital fingerprint. If they would have just made an MD5 image, that would have been fine and I could have had a digital fingerprint to compare it to the data in the EnCase image. They didn't do that. It wasn't the FBI that didn't do it, it was Mark Hansen that didn't do it. The FBI just imaged bad stuff already that had been destroyed. So I can't take the Acronis, the data out of the Acronis image that does not have a starting point and compare it to something with a known starting point, other than to say it wouldn't match.

RT 143, 144-45.[40]

Given the deficiencies associated with the Acronis back-up copy software, the FBI's failure to take action to secure custody of the Wu laptop notwithstanding knowledge that Hoffman had directed Wu to return to Portland, the damage inflicted by Hansen's activities with respect to loading the Acronis software onto the Wu laptop,[41] the damage and spoliation caused by Hoffman's manipulation of the Wu laptop, the apparent breach in the chain of custody between the date the Wu laptop and the Hansen USB external drive were taken into custody by the FBI (October 20-21, 2006) and the date those items were logged into evidence (November 1, 2006),[42] the apparent calibration error with respect to the NWRCFL's imaging equipment,[43] the government's failure to identify the standards and protocols employed in the creation of the FTK EnCase images,[44] and the fact that the

[40] As previously noted, the government's witness, NWRCFL Operations Manager Steven Johns, testified that he would not use the Acronis backup software to make a forensic image. RT 164.

[41] "More generally, electronically stored information is more easily and more thoroughly changeable than paper documents. Electronically stored information can be modified in numerous ways that are sometimes difficult to detect without computer forensic techniques. Moreover, the act of merely accessing or moving electronic data can change it. For example, booting up a computer may alter data contained on it. Simply moving a word processing file from one location to another may change creation or modification dates found in the metadata." The Sedona Conference, *The Sedona Principles: Best Practices Recommendations for Addressing Electronic Document Production* (Johnathan M. Redgrave *et al* eds., 2d ed. 2007), at p. 3.

[42] Operations Manager Johns testified that he did not know who had possession of the Wu laptop and the Acronis back-up copy USB external drive device between October 20, 2006 and November 1, 2006. RT 159-60.

[43] The creation date of the FTK EnCase Acronis image is October 3, 2006; the creation date of the FTK EnCase Wu laptop image is October 5, 2006. *See* Declaration Of Computer Forensics Expert Michael A. Bean In Support Of Motion To Exclude Images Of The Wu Laptop Hard-Drive [Docket No. 36], at pp. 6-7.

[44] The government failed to identify the protocols and procedures utilized by the FBI in creating the FTK Encase Wu Laptop and Acronis backup copy images, notwithstanding Forensic

FTK EnCase image of the Wu Laptop could only produce an image of an already compromised computer hard drive,[45] there are simply no facts whereby this Court may find that the "process or system" used to produce the FTK EnCase Wu laptop and Acronis back-up copy images produced an accurate result (*i.e.*, that these images accurately reproduced the entirety of the electronic data that existed on the Wu Laptop prior to its seizure).

C. The Extensive Spoliation Of The Electronic Data Content Of The Wu Laptop Precludes Any Valid Determination By This Court With Respect To The Authentication Of The Electronic Data Content Of The FTK Encase Wu Laptop Image.

Proof of facts adequate to assure the continuing integrity of the electronic data content on the Wu Laptop is essential to the authentication of that content. During the motion hearing, testimony that the Wu Laptop had been subjected to intrusive manipulation by Hansen and Hoffman was

Computer Expert Bean's testimony that the FBI's imaging computer or computers were not properly calibrated. AUSA Nyhus made several contradictory statements concerning the use of protocols by the FBI in conducting a forensic examination of the contents of a computer and/or in making a forensic image of a computer hard drive. Initially, AUSA Nyhus represented to the Court that "[t]here is no set protocol for examination or extraction of evidence in every case." RT 9. However, AUSA Nyhus also stated that "[t]here is a practice and procedure within the FBI that's maintained by the National Program Office. Quantico manages that material as it trains its agents." RT 9. According to NWRFCL Operations Manager Johns, the laboratory obtained its standard operating procedures from the Digital Evidence Laboratory at Quantico, Virginia. RT 172-73. However, no testimony as regards compliance with preset protocols by the FBI in creating the laptop hard drive and Acronis backup copy images was adduced by the government, nor did FBI Special Agent Joel Brillhart, the agent who made the images, testify.

[45] In his cross-examination of Forensic Computer Expert Bean, AUSA Nyhus characterized the conclusion to be drawn from Bean's evaluation of the FTK EnCase Wu laptop and Acronis back-up copy images as follows:

Q. **So what this amounts to really is that the FBI imaged bad stuff?**

A. **Yes, sir.**

RT 153 (emphasis added).

received. The government failed to rebut this testimony and failed to provide proof of any foundational facts sufficient to enable this Court to find that a reasonable jury could make a determination that the contents of the Wu Laptop, prior to its seizure on October 17, 2006, and the contents of either of the FTK EnCase images are identical.

When issues arise as to the integrity of electronic data, Weinstein's treatise is clear as to the proof required:

> Files stored in a computer hard drive or a diskette are subject to manipulation and corruption unless proper safeguards are taken . . .. Accordingly, if documents are produced or seized in an electronic format, a proper authentication foundation must show both what the evidence was when gathered and that it has remained unchanged since then. A foundation similar to a "chain of custody" that accounts for each step at which a change to the evidence might occur will satisfy an objection that files in a computer hard drive or diskette are not authentic.

5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* §900.07[2][b] (2d ed. 2005).

Hoffman's manipulation of the Wu laptop while it was in his possession resulted in spoliation.[46] Although Hoffman claimed he did not delete any files, his commission of tariff fraud with respect to The Hoffman Group products he was importing into the United States from China discloses that he had a motive to secret and suppress information pertaining to his criminal violation of U.S. import tax laws. The 2005 Outlook e-mail communications between Hoffman and

[46] Forensic Computer Expert Bean found that, following the seizure of the Wu laptop, over a thousand files on the laptop's hard drive had either been created, accessed or written to. RT 128. The manner in which the Wu laptop was manipulated and used following its seizure "degraded the amount of unallocated cluster data" that Bean had to work with. RT 129. Bean also found files in the FTK EnCase Acronis backup copy image that he did not find in the FTK EnCase Wu laptop image, again confirming that deletion of files had occurred. RT 123-24. The law of spoliation of electronic evidence and remedies for spoliation are discussed in Mr. Khoo's Reply To Government's Response To Motion To Exclude Images Of The Wu Laptop Hard-Drive And Request For Immediate Production Of Information Relevant To Determination Of Pending Motions [Docket No. 78], at pp. 14-16.

Richard X, submitted as Defendant Khoo's Exhibits 6 and 7, also involved Wu. Forensic Computer Specialist Bean was asked to search the FTK EnCase Wu laptop image for Outlook e-mail files for the time periods 2005 and 2006. RT 127. He was able to locate only a single Hoffman 2006 .PST file in deleted space. RT 127. He was not able to determine when this file had been deleted. Hoffman also denied employing the defrag utility while the Wu laptop was in his possession. RT 64-65. However, Bean's determination that the defrag utility had been run at approximately 8:44 p.m. on October 17, 2006, contradicts Hoffman's denial. RT 131.[47]

Authentication issues implicate Federal Rule of Evidence 104(b)'s "relevancy conditioned on fact" provision which provides that "[w]hen the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition."[48] In accordance with Rule 104(b), in the face of a challenge to the authenticity of evidence, a trial court must make a preliminary ruling as to the sufficiency of the evidence to enable a reasonable jury to ultimately

[47] In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 504 n.14 (D.Md. 2010), Magistrate Judge Grimm observed: "[I]t is foreseeable that the running of a disk defragmentation program colloquially referred to as 'defragging,' can result in the loss of the files that were recoverable before the defragmentation occurred."

[48] The "fulfillment of the condition" in the instance of the FTK Wu laptop and Acronis backup copy images is that the data content of those images represents a complete reproduction of the physical data content of the Wu Laptop as it existed on October 17, 2006. In other words, the government must establish that the FTK Wu laptop and Acronis backup copy images are "duplicates" of the Wu Laptop – *i.e.* that they are "counterparts" which "accurately reproduce[] the original." *See* Federal Rule of Evidence 1001(4). In this regard , it is pertinent to note that Federal Rule of Evidence 1003 provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Further discussion of the extent to which the afore-referenced images fail to qualify as duplicates of the original Wu laptop computer is set forth in the Memorandum Of Points And Authorities In Support Of Motion To Exclude Images Of The Wu Laptop And External Hard Drive [Docket No. 35], at pp. 21-24.

resolve the authentication issue. 5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* §900.06[1][c][i] (2d ed. 2005). As the Ninth Circuit declared in *United States v. Gil*, 58 F.3d 1414, 1419-1420 (9th Cir. 1995):

> To find that the ledgers constituted admissions, there must be sufficient evidence to enable the jury to decide that the defendants authored or adopted the ledgers. *See* Fed.R.Evid. 801(d)(2)(A) & (B). When evidence is admitted subject to the jury's finding that a threshold condition is satisfied, "[t]he judge makes a preliminary determination whether the foundation evidence is sufficient to support a finding of fulfillment of the condition." Fed.R.Evid. 104(b) advisory committee's note; see *United States v. Reilly*, 33 F.3d 1396, 1404-05 (3rd Cir.1994) ("[O]nce the court finds that evidence has been introduced sufficient to permit a reasonable juror to find that the matter in question is what its proponent claims, a sufficient foundation for introduction in evidence has been laid."); *United States v. Monks*, 774 F.2d 945, 950 (9th Cir.1985) (holding that before introducing evidence as an adoptive admission, "the district court must first find that sufficient foundational facts have been introduced for the jury reasonably to conclude that the defendant did actually hear, understand and accede to the statement").

The "key purpose of authentication is to ensure that only genuine and trustworthy evidence is considered." 5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* §900.06[1][a] (2d. ed. 2005). Although the authentication determination is a preliminary determination, it is still the case that it is the Court's duty to act as a "gatekeeper" and exclude evidence that does not bear sufficient indicia of trustworthiness. *In re Vee Vinhnee*, 336 B.R. at 443.[49]

[49] Rule 104(b) does not explicitly establish the amount of proof necessary to make a preliminary finding with respect to the facts requisite to authenticate an item of evidence. According to Weinstein,

> Ordinarily, a judge may - as a condition precedent to admission - make a preliminary finding merely on a prima facie showing that "the matter in question is what its proponent claims." Under this standard, a judge need only determine that a reasonable juror could find that the evidence is genuine and what its proponent claims it to be."

5 Joseph M. McLoughlin ed., *Weinstein's Federal Evidence* §900.06[1][c][ii] (2d. ed. 2005). Mr. Khoo contends that, given the nature of the evidence (as involving computers and complex

Genuine questions as to the authenticity of the data content of the FTK EnCase Wu laptop and Acronis backup copy images have been raised. It was therefore incumbent on the government at the November 16 hearing, to submit such evidence as to the foundational facts as would enable a reasonable jury to determine "that the record reproduced from the electronic media is identical to the record that was originally stored." *In re Vee Vinhee*, 336 B.R. at 449. The government wholly failed to adduce any facts to meet its burden of proof in this regard.

CONCLUSION

A "fair trial in a fair tribunal is a basic requirement of due process." *In re Murchison*, 349 U.S. 133, 136 (1955). Federal Rule of Evidence 102 states that the rules of evidence "shall be construed to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined."

In the course of pleading grounds for exclusion of the FTK EnCase images of the Wu laptop computer, and during the motion hearing of November 16, 2010, Mr. Khoo has demonstrated that: (1) the Acronis backup copy was made using software that has not been approved for forensic imaging use; (2) spoliation of the Wu laptop hard drive commenced with Hansen's use of the Acronis software and continued through Hoffman's two/three day rummaging around in the contents of the Wu laptop hard drive; (3) analysis of the FTK EnCase image of the Wu Laptop hard drive discloses that thousands of files were added, altered and/or created after the lap top was seized by

technological questions), a clear and convincing evidence standard should be employed in the authentication determination. *See* Reply To Government's Response To Motion To Exclude Images Of The Wu Laptop Hard-Drive And Request For Immediate Production Of Information Relevant To Determination Of Pending Motions [Docket No. 78], at pp. 7-9.

Hoffman; (4) analysis of the FTK EnCase image of the Wu Laptop hard drive discloses that its unallocated disk space contains thousands of deleted files that cannot be recovered, and for which the date of deletion cannot be determined; (5) that files were deleted from the Wu laptop after the Acronis software was installed and run; (6) that a defrag utility was run while the lap top was in Hoffman's possession; (7) that Hoffman had a motive to delete files and run the defrag utility in order to delete e-mail and hide his criminal activity in avoiding U.S. tariffs on products imported from China; (8) that there is an unexplained breach in the chain of custody between the time Hoffman turned over the Wu Laptop and the Hansen USB device to SA Slinkard (October 20-21, 2006) and the date that those items were logged into evidence at the NWRFCL facility (November 1, 2006); and (9) that the NWRFCL's imaging equipment had not been properly calibrated at the time the FTK EnCase images were made.

The requirements of authentication as a precondition to admissibility may not be great, but they nonetheless exist as the hinge to the gate that this Court, as gatekeeper, must not swing open unless and until sufficient trustworthy evidence as to the appropriateness of substituting the FBI's forensic images for the original data content of the Wu laptop has been adduced by the government. The government was given its day in Court on November 16, 2010, to make such a showing of trustworthiness. It failed to do so. The FTK EnCase images and the data content of those images should be declared inadmissible at trial in this case.

Respectfully submitted this January 14, 2011.

/s/ Christopher J. Schatz
Christopher J. Schatz
Attorney for Defendant Hock Chee Khoo